

AddAccess-ACE

Access Control Entries not inheritable

Sean Barnum, Cigital, Inc. [[vita](#)¹]

Copyright © 2005 Cigital, Inc.

2005-10-03

"Original Cigital Coding Rule in XML"

Mime-type: text/xml, #####: 4395 bytes

Identification Difficulty

Scan

Priority

Medium

Attack Categories

- Privilege Exploitation

Vulnerability Categories

- Access Control

Software Context

- Security

Description

When an access control entry (ACE) is added via `AddAccessAllowedAce()` or `AddAccessDeniedAce()`, this entry is not inheritable, which can create a vulnerability to attack if inheritance is assumed. The `AddAccessAllowedAce` function adds an access-allowed ACE to an access control list (ACL). The access is granted to a specified security identifier (SID). The `AddAccessDeniedAce` function adds an access-denied ACE to an ACL. The access is denied to an SID. The ACE added by `AddAccessDeniedAce` is not inheritable. This can lead to subclasses not being denied access when they should be.

Application Programming Interfaces

-
1. `daisy:35` (Barnum, Sean)

Function Name	Comments
AddAccessAllowedAce	
AddAccessDeniedAce	

Method of Attack

If AddAccessDeniedAce is used to restrict access to an object, then the access restriction will not propagate any child objects. If the restriction should have been propagated to the children, then access rights for the children will be more permissive than was intended, and an attacker could exploit this.

Solutions

Applicability	Description	Efficacy
Whenever adding an ACE.	To control whether the new ACE can be inherited by child objects, use the AddAccessAllowedAceEx or AddAccessDeniedAceEx function.	Effective, given appropriate thought as to proper access permissions.

Signature Details

```

BOOL AddAccessAllowedAce(PACL pAcl, DWORD dwAceRevision, DWORD AccessMask, PSID pSid);
BOOL AddAccessDeniedAce(PACL pAcl, DWORD dwAceRevision, DWORD AccessMask, PSID pSid);

```

Examples of Incorrect Code

- Example 1

```

if (! AddAccessDeniedAce( pAcl, dwAceRevision, AccessMask, pSid) {
    /* handle error */
}

```

Examples of Corrected Code

- Example 1

```

DWORD AceFlags = OBJECT_INHERIT_ACE; // Inheritance flags should be set as
appropriate
if (! AddAccessDeniedAceEx( pAcl, dwAceRevision, AceFlags, AccessMask, pSid) {
    /* handle error */
}

```

Source References

- Howard, Michael & LeBlanc, David C. Writing Secure Code, 2nd ed. Redmond, WA: Microsoft Press, 2002, ISBN: 0735617228., p.409

Recommended Resources

Resource	Link
MSDN reference for AddAccessAllowedAce	http://msdn.microsoft.com/library/default.asp?url=/library/en-us/secauthz/security/addaccessallowedace.asp ²
MSDN reference for AddAccessDeniedAce	http://msdn.microsoft.com/library/default.asp?url=/library/en-us/secauthz/security/addaccessdeniedace.asp ³

Discriminant Set

Operating Systems

- Windows

Languages

- C
- C++

Cigital, Inc. Copyright

Copyright © Cigital, Inc. 2005. Cigital-authored documents are sponsored by the U.S. Department of Defense under Contract FA8721-05-C-0003. Cigital retains copyrights in all material produced under this contract. The U.S. Government retains a non-exclusive, royalty-free license to publish or reproduce these documents, or allow others to do so, for U.S. Government purposes only pursuant to the copyright license under the contract clause at 252.227-7013.

Permission to reproduce this document and to prepare derivative works from this document for internal use is granted, provided the copyright and “No Warranty” statements are included with all reproductions and derivative works.

For information regarding external or commercial use of copyrighted materials owned by Cigital, including information about “Fair Use,” contact Cigital at copyright@cigital.com¹.

####

###	#####
Copyright Holder	Cigital, Inc.

2. <http://msdn.microsoft.com/library/default.asp?url=/library/en-us/secauthz/security/addaccessallowedace.asp>

3. <http://msdn.microsoft.com/library/default.asp?url=/library/en-us/secauthz/security/addaccessdeniedace.asp>

1. <mailto:copyright@cigital.com>

####

###	#####
Attack Categories	Privilege Exploitation
Operating System	Windows
Software Context	Security
Vulnerability Categories	Access Control